UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

YVON HANEKOM and KADE MCCRAW, individually and on behalf of all others similarly situated, Plaintiffs, v. MANAGED CARE OF NORTH AMERICA, INC., d/b/a MCNA DENTAL, Defendant.	Case No. 0:23-cv-61151 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Yvon Hanekom and Kade McCraw (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, by and through undersigned counsel, bring this Class Action Complaint against Defendant Managed Care of North America, Inc. (d/b/a MCNA Dental) ("MCNA" or "Defendant"), an in support thereof allege as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members")—totaling approximately 8.9 million people—who had their sensitive personal identifiable information ("PII") and protected health information ("PHI")—as defined by Health Insurance Portability and Accountability Act ("HIPPA")—disclosed to unauthorized third parties that accessed and removed the PII and PHI from MCNA's system between at least February 26 and March 7, 2023[1], if not longer (the "Data Breach").

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited June 14, 2023).

2. MCNA advertises itself as "a leading dental benefits manager committed to providing high quality services to state agencies and managed care organizations for their Medicaid, Children's Health Insurance Program (CHIP), and Medicare members."[2] MCNA's website states "MCNA provides a full range of dental benefits management services including:

- Primary and Specialty Care Dental Network
- Member Services
- Provider Relations
- Claims
- Enrollment
- Quality Assurance and Improvement
- Risk Management
- Credentialing
- Compliance"[3]

3. MCNA sent letters to Plaintiffs and Class Members on or about May 26, 2023 ("Notice Letter"), notifying them of the Data Breach and stating that their names, addresses, dates of birth, Social Security numbers, driver's licenses numbers, and/or other government-issued ID numbers ("PII"), as well as their health insurance plan information, insurance companies, member numbers, Medicaid-Medicare ID numbers, medical/dental bills and insurance claims, and other dental services and health information ("PHI"), were compromised in the Data Breach.[4] The compromised information includes sensitive medical records/information related to dental care and visits such as care for teeth or braces, dental visits, dentist name, doctor name, past care, x-rays/photographs, medicines and medications, and other forms of treatment.

[2] https://www.mcna.net/en/company-overview (last visited June 14, 2023).
[3] https://www.mcna.net/en/technology (last visited June 14, 2023).
[4] A sample draft of MCNA's Notice Letter is accessible at: https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 14, 2023).

4. It has been reported that the Data Breach was a ransomware attack conducted by the notorious Russia-linked ransomware group, LockBit, which claims to have committed the Data Breach.[5] LockBit claims to have requested a $10 million ransom from MCNA and when MCNA refused to pay the ransom, LockBit published all of the files it exfiltrated from MCNA's systems.[6] Because the Data Breach was conducted by known, self-proclaimed ransomware hackers, Plaintiffs' and Class Members' sensitive PII and PHI are irrefutably in the possession of known bad actors.

5. MCNA's Notice Letter states that it discovered the Data Breach on March 6, 2023, but MCNA did not notify impacted individuals—such as Plaintiffs and Class Members—of the Data Breach for 81 days, until May 26, 2023. MCNA's 81-day delay runs afoul of promises on its website that "[MCNA is] required by law to maintain the privacy and security of your protected health information. [MCNA] will let you know promptly if a breach occurs that may have compromised the privacy or security of your information,"[7] and "[i]n the event of a data breach, MCNA shall promptly notify any possibly affected [individuals]."[8]

6. MCNA reported on the Maine Attorney General's website that on May 26, 2023, it sent written notification to 8,923,662 individuals that it suffered the Data Breach and informed them that their PII and PHI was compromised thereby.[9] According to MCNA's Notice Letter, on May 3, 2023, MCNA discovered "that an unauthorized party was able to access certain MCNA systems …. and remove copies of some personal information between February 26, 2023 and

---

[5] https://techcrunch.com/2023/05/31/ransomware-attack-on-us-dental-insurance-giant-exposes-data-of-9-million-patients/?guccounter=1 (last visited June 14, 2023).
[6] *Id.*
[7] https://www.mcna.net/en/privacy (last visited June 14, 2023).
[8] https://www.mcna.net/en/privacy-statement (last visited June 14, 2023).
[9] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited June 14, 2023).

March 7, 2023."[10] The Data Breach resulted from MCNA's failure to adequately protect and safeguard the highly sensitive PII and PHI entrusted to it.

7. Notably, MCNA's Notice Letter makes no mention that the Data Breach involved a ransomware attack, of the ransom demanded by LockBit, or MCNA's refusal to pay as little as $1.12 per impacted person to prevent LockBit from publishing their highly sensitive PII and PHI.

8. MCNA owed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. MCNA breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII/PHI entrusted to it from unauthorized access and disclosure.

9. As a result of MCNA's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class Members' PII and PHI was accessed and disclosed by an unauthorized actor. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all similarly situated individuals whose PII and/or PHI was exposed as a result of the Data Breach, which MCNA learned of on or about May 3, 2023, but did not publicly disclose until May 26, 2023.

10. Plaintiffs, on behalf of themselves and all other Class Members, asserts claims for negligence, negligence per se, unjust enrichment, and breach of fiduciary duty, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

[10] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 12, 2023).

PARTIES

A. Plaintiff Yvon Hanekom

11. Plaintiff Yvon Hanekom ("Plaintiff Hanekom") is a resident and citizen of the state of Alabama and resides in Axis, Alabama.

12. On or about May 26, 2023, MCNA sent Plaintiff Hanekom a letter confirming that his PII and PHI was impacted by the Data Breach. In the letter, MCNA identified that the nature of the information involved includes Plaintiff Hanekom's name, address, date of birth, Social Security number, driver's license number or other government-issued ID number, health insurance plan information, insurance companies, member numbers(s), Medicaid-Medicare ID number(s), medical/dental bills and insurance claims, sensitive medical records/information related to dental care and visits such as care for teeth or braces, dental visits, dentist name, doctor name, past care, x-rays/photographs, medicines and medications, and other forms of treatment.

13. In the letter MCNA sent Plaintiff Hanekom, it stated that the Data Breach occurred between February 26 and March 7, 2023. Two days after the date of the Data Breach, Plaintiff Hanekom received a letter stating that someone submitted a fraudulent insurance claim for dental work in his name.

14. Prior to retaining counsel for claims related to the data breach, Plaintiff Hanekom spent at least ten hours investigating the fraudulent claim for dental work that was submitted in his name, and otherwise monitoring his accounts for fraudulent activity. He will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

B. Plaintiff Kade McCraw

15. Plaintiff Kade McCraw ("Plaintiff McCraw") is a resident and citizen of the state

of Massachussetts and resides in Springfield, Massachussetts.

16. On or about May 26, 2023, MCNA sent Plaintiff McCraw a letter confirming that his PII and PHI was impacted by the Data Breach. In the letter, MCNA identified that the nature of the information involved includes Plaintiff Hanekom's name, address, date of birth, Social Security number, driver's license number or other government-issued ID number, health insurance plan information, insurance companies, member numbers(s), Medicaid-Medicare ID number(s), medical/dental bills and insurance claims, sensitive medical records/information related to dental care and visits such as care for teeth or braces, dental visits, dentist name, doctor name, past care, x-rays/photographs, medicines and medications, and other forms of treatment

17. Only approximately two weeks after the Data Breach, Plaintiff McCraw experienced a fraudulent transaction on Walmart.com on March 22, 2023, on his CapitalOne credit card. Plaintiff McCraw called CapitalOne to dispute the fraudulent transaction, his card was closed, and he was mailed a replacement credit card. Approximately 5-7 days later, Plaintiff McCraw was alerted that another fraudulent transaction was attempted on his same CapitalOne account.

18. Prior to retaining counsel for claims related to the data breach, Plaintiff McCraw has spent approximately six hours investigating the fraudulent transaction on his CapitalOne account, contacting CapitalOne about the transaction, contacting Experian to check his credit, and otherwise monitoring his accounts for fraudulent activity and will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

C. Defendant Managed Care of North America, Inc. (d/b/a MCNA Dental)

19. Defendant MCNA is a Florida corporation with its principal place of business in Miramar, Florida. MCNA Dental's headquarters are located at 3100 SW 145th Avenue, Suite #200, Miramar, Florida 33027.[11]

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more Class Members are citizens of states different from Defendant.

21. The Court has personal jurisdiction over Defendant because it maintains its principal place of business in this judicial district, conducts significant business in Florida, and/or otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Florida.

22. Venue properly lies in this district because, *inter alia*, Defendant maintains its principal place of business in this judicial district; transacts substantial business, has agents, and is otherwise located in this district; and/or a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this judicial district.

---

11 https://search.sunbiz.org/Inquiry/CorporationSearch/SearchResultDetail?inquirytype=EntityName&directionType=Initial&searchNameOrder=MANAGEDCARENORTHAMERICA%20S505840&aggregateId=domp-s50584-cfa68dbb-783d-4706-b6dc-6e2d533ab84a&searchTerm=Managed%20Care%20of%20North%20America&listNameOrder=MANAGEDCARENORTHAMERICA%20S505840 (last visited June 14, 2023).

FACTUAL ALLEGATIONS

A. Overview of Defendant

23. MCNA touts itself as "a leading dental benefits manager committed to providing high quality services to state agencies and managed care organizations for their Medicaid, Children's Health Insurance Program (CHIP), and Medicare members," and "also offers dental plans for private employers, individuals, and families."[12]

24. MCNA's website states that it provides the following services:

> MCNA provides a full range of dental benefits management services including:
>
> - Primary and Specialty Care Dental Network
> - Member Services
> - Provider Relations
> - Claims
> - Enrollment
> - Quality Assurance and Improvement
> - Risk Management
> - Credentialing
> - Compliance[13]

25. Discovery will show that through its provision of the foregoing services, MCNA obtains possession of patients'—such as Plaintiffs' and Class Members'—highly sensitive PII and PHI. Thus, in the regular course of its business, MCNA collects and maintains the PII and PHI of (1) its insureds, and/or (2) patients/subscribers/insureds/customers of healthcare professionals, managed care organizations, and/or state agencies that used MCNA's services, as well as their parents, guardians, or guarantors, and other individuals. That information ordinarily includes: (1) patient demographic information (such as patient name, guarantor name, parent/guardian name, address, email address, and date of birth); (2) Social Security Numbers ("SSNs"),

[12] https://www.mcna.net/en/company-overview (last visited June 14, 2023).
[13] https://www.mcna.net/en/technology (last visited June 14, 2023).

(3) driver's license numbers or other state-issued ID numbers, (4) insurance information (payer name, payer contract dates, policy information including type and deductible amount and subscriber number); (5) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (6) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by your provider); and (7) information of a parent, guardian, or guarantor. Defendant stores this information digitally.

26. MCNA's website is replete with representations that MCNA has systems and processes in place to ensure the safety and privacy of PII and PHI entrusted to it. For instance, MCNA's website claims that it uses proprietary technology to protect data in its possession: "MCNA Dental manages enrollment, provider network, claims handling, and other operations data **on a fully integrated proprietary management information system** (MIS) called DentalTrac™."[14]

27. Moreover, MCNA's website informs consumers and viewers that it has conducted independent, third-party audits of its systems and processes to ensure that they are adequate to safeguard data in its possession, which includes PII and PHI: "MCNA has successfully completed an independent, third-party SOC 2 audit of the processes and controls that ensure the security and availability of our information management systems and data."[15] MCNA's website states further:

> We have successfully completed an independent, third-party SOC 2 audit by the AICPA of the processes and controls that ensure the security and availability of our information management systems and data. These certifications underscore our continuous commitment to operating under the highest quality standards in our industry and to ensuring the best service possible for our members, providers, and clients.[16]

[14] *Id*.
[15] *Id*.
[16] https://www.mcna.net/en/company-overview (last visited June 14, 2023).

28. The SOC 2 audit touted on MCNA's website is designed specifically to ensure adequate data privacy and confidentiality:

> "These reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.[17]

29. MCNA promises consumers and website viewers that it takes steps to ensure their sensitive PII and PHI entrusted to it is safe:

> MCNA takes pride in the fact that we are recognized leaders in the dental benefits industry. One of our strengths is our ability to administer dental plans in an effective and innovative manner **while safeguarding our members' protected health information**. We are committed to complying with the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We demonstrate our commitment through our actions. **MCNA has implemented company-wide policies and procedures to comply with the provisions of HIPAA**. We regularly conduct employee training and education in relation to HIPAA requirements to **ensure those policies and procedures are in use**.[18]

30. Thus, MCNA tells consumers and website viewers that its "services and programs are built to meet and exceed industry standards and best practices …. to ensure that MCNA offers exceptional services that meet all industry standards of care."[19]

31. Furthermore, on its website, MCNA recognizes that it has a legal duty to safeguard sensitive PII and PHI entrusted to it[20]:

> ## What is MCNA's Legal Duty regarding the notice of privacy practices?
>
> **The law says MCNA has to keep your health information private**. We have to give you this notice about our privacy practices, our legal duties and your rights. **We must follow the privacy practices that are in this notice**.

[17] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report (last visited June 14, 2023).
[18] https://www.mcna.net/en/privacy (last visited June 14, 2023).
[19] https://www.mcna.net/en/company-overview (last visited June 14, 2023).
[20] https://www.mcna.net/en/privacy (last visited June 14, 2023).

> ## What are MCNA's responsibilities regarding my health information?
> **We are required by law** to maintain the privacy and security of your protected health information.

32. Again, MCNA assures consumers and website viewers that it safeguards their and PHI[21]:

> ## What is personal health information?
> Personal health information includes both medical information and individually identifiable information, like your name, address, telephone number, or Social Security number. This information is created or received by a healthcare provider or health plan that relates to your physical or mental health or condition, providing healthcare to you, or the payment for such healthcare. **We protect this information in all formats including electronic, written and oral information**.

33. MCNA claims that it has safeguards in place to ensure the privacy, confidentiality, and protection of PHI entrusted to it, and that those safeguards comply with federal and state laws[22]:

> ## How do we protect your information?
> **In keeping with federal and state laws** and our own policy, we have a responsibility to protect the privacy of your information. **We have safeguards in place to protect your information** in various ways including:
>
> - Limiting who may see your information and how we use or disclose your information.
> - Informing you of our legal duties about your information.
> - Training our employees and associates about company privacy policies and procedures.

34. Likewise, MCNA's website acknowledges that it has a duty to ensure the confidentiality and privacy of PII entrusted to it, and assures consumers and website viewers that it has systems and processes in place to do so[23]:

---

[21] *Id*.
[22] *Id*.
[23] https://www.mcna.net/en/privacy-statement (last visited June 14, 2023).

> We have the important responsibility to protect the security of the personal information we collect from you.
>
> * * *
>
> **Personal Information**
>
> MCNA may collect personal information about you in order to provide you with information, products, and services through our website. This personal information may include, but is not limited to, your name, address, and social security number. It may include financial information that you voluntarily supply when you register or initiate transactions. We may also collect non-personal information about how you navigate through the website.

35. Despite the Data Breach, MCNA assures consumers and website viewers that it has systems and processes in place to prevent the precise type of unauthorized access that occurred in the Data Breach[24]:

> **Security and Confidentiality**
>
> **Our Sites have security measures in place to protect the loss, misuse, and alteration of the information under our control**. Our Sites use Secure Sockets Layer (SSL) for transmitting private documents over the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection. The web browsers Mozilla Firefox, Apple Safari, Chrome, and Internet Explorer support SSL. Many websites use this protocol to obtain confidential user information, like credit card numbers.
>
> **MCNA also uses a firewall to prevent unauthorized access**. All messages entering or leaving our Sites pass through the firewall, which examines each of them. It blocks those that do not meet the specified security criteria. As effective as SSL and firewalls are, though, no security system is impenetrable.

36. As evidenced by, *inter alia*, their receipt of the Notice from MCNA informing them that their PII and PHI were compromised in the Data Breach, Plaintiffs and Class Members are, or were, MCNA's insureds or patients of healthcare professionals, managed care organizations, and/or state agencies that used MCNA's services, and thereby entrusted MCNA with their PII and/or PHI, from which MCNA profited.

[24] *Id.*

37. Yet, contrary to MCNA's website representations—by virtue of MCNA's admission that it experienced the Data Breach which revealed the PII and PHI of nearly 9 million individuals—MCNA did not have adequate measures in place to protect and delete sensitive PII and PHI entrusted to it. Instaed, MCNA's website wholly fails to disclose the truth: that MCNA lacks sufficient processes to protect the PII and PHI that is entrusted to it.

B. The Data Breach

38. MCNA's Notice Letter disclosing the Data Breach states that on March 6, 2023, MCNA discovered "that an unauthorized party was able to access certain MCNA systems …. and remove copies of some personal information between February 26, 2023 and March 7, 2023."[25] Thus, known, malicious, unauthorized cybercriminals had access to MCNA's systems—and Plaintiffs' and Class Members' sensitive PII and PHI stored thereon—for at least ***ten consecutive days straight***, from at least February 26 through March 7, 2023, if not longer.

39. Thus, the Data Breach resulted from MCNA's failure to adequately protect and safeguard the highly sensitive PII and PHI entrusted to it.

40. MCNA's Notice Letter states that it discovered the Data Breach on March 6, 2023, but MCNA did not notify impacted individuals—such as Plaintiffs and Class Members—of the Data Breach for ***81 days***, until May 26, 2023.

41. MCNA's 81-day delay is contrary to multiple promises on its website that "[MCNA is] required by law to maintain the privacy and security of your protected health information. [MCNA] will let you know promptly if a breach occurs that may have compromised the privacy

[25] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 12, 2023).

or security of your information,"[26] and "[i]n the event of a data breach, MCNA shall promptly notify any possibly affected [individuals]."[27]

42. MCNA reported on the Maine Attorney General's website that on May 26, 2023, it sent written notification to 8,923,662 individuals that it suffered the Data Breach and informed them that their PII and PHI was compromised thereby.[28]

43. MCNA's Notice Letter sent to those 8,923,662 individuals impacted by the Data Breach—such as the one received by Plaintiffs—stated that their PII and PHI that was compromised in the Data Breach included their names, addresses, dates of birth, Social Security numbers, driver's licenses numbers, and/or other government-issued ID numbers, as well as their health insurance plan information, insurance companies, member numbers, Medicaid-Medicare ID numbers, medical/dental bills and insurance claims, and other dental services and health information, were compromised in the Data Breach.[29] The compromised information includes sensitive medical records/information related to dental care and visits such as care for teeth or braces, dental visits, dentist name, doctor name, past care, x-rays/photographs, medicines and medications, and other forms of treatment.[30]

---

[26] https://www.mcna.net/en/privacy (last visited June 14, 2023).
[27] https://www.mcna.net/en/privacy-statement (last visited June 14, 2023).
[28] https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56.shtml (last visited June 14, 2023).
[29] A sample draft of MCNA's Notice Letter is accessible at: https://apps.web.maine.gov/online/aeviewer/ME/40/895b95c8-abc8-41f1-8c3f-b0415575de56/871548ce-318e-48dd-a3b9-6eec9ef88da9/document.html (last visited June 14, 2023).
[30] *Id*.

44. It has been reported that the Data Breach was a ransomware attack conducted by the notorious Russia-linked ransomware group, LockBit, which claims to have committed the Data Breach.[31]

45. LockBit first surfaced in September 2019 and since then has been linked to a number of massive, high-profile ransomware attacks such as: (1) the United Kingdom postal company, Royal Mail[32]; (2) the financial software company, Ion Group[33]; and (3) California's Department of Finance[34].

46. Due to its malicious conduct in executing major ransomware attacks, LockBit has been the target on criminal investigations and charges. In November 2022, one of its leaders, a dual Russian-Canadian citizen, Mikhail Vasiliev, was arrested in Canada.[35] Likewise, in March 2023, the United States government announced that it had indicted a Russian national accused of being a key figure in the LockBit rnasomeware group.[36]

47. LockBit claims to have requested a $10 million ransom from MCNA and when MCNA refused to pay the ransom, LockBit published all of the files it exfiltrated from MCNA's systems.[37]

---

[31] https://techcrunch.com/2023/05/31/ransomware-attack-on-us-dental-insurance-giant-exposes-data-of-9-million-patients/?guccounter=1 (last visited June 14, 2023).

[32] https://techcrunch.com/2023/02/14/royal-mail-refused-to-pay-absurd-lockbit-ransom-chat-logs-say/ (last visited June 14, 2023).

[33] https://techcrunch.com/2023/02/02/ion-group-lockbit-derivatives-ransomware/ (last visited June 14, 2023).

[34] https://techcrunch.com/2022/12/13/california-finance-department-lockbit-ransomware/ (last visited June 14, 2023).

[35] https://techcrunch.com/2022/11/10/police-arrest-suspected-lockbit-operator-as-the-ransomware-gang-spills-new-data/ (last visited June 14, 2023).

[36] https://techcrunch.com/2023/05/16/doj-sanctions-matveev-wazawaka-ransomware/ (last visited June 14, 2023).

[37] *Id*.

48. A listing on LockBit's website suggests that it has up to 700 gigabytes of data that the ransomware group illegally exfiltrated from MCNA's systems.[38]

49. LockBit uploaded that information—comprised of Plaintiffs' and Class Members' highly sensitive PII and PHI—to its website on April 7, 2023 and listed it for sale on the dark web. Yet MCNA waited nearly two months after that date before notifying impacted individuals of the Data Breach.[39]

50. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiffs' and Class Members' sensitive PII and PHI are irrefutably in the possession of known bad actors. Furthermore, Plaintiffs' and Class Members' PII and PHI is already listed for sale on the dark web, which places them at imminent risk that it will be misused.

51. Remarkably, noticeably absent from MCNA's Notice Letter is any mention, whatsoever, that the Data Breach involved a ransomware attack, of LockBit, of the ransom demanded by LockBit, of MCNA's refusal to pay as little as $1.12 per impacted person to prevent LockBit from publishing their highly sensitive PII and PHI, or that impacted individuals' highly sensitive PII and PHI is already for sale on the dark web.

52. As explicitly acknowledged and stated on its own website, MCNA owed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure, and to promptly notify individuals of a data breach involving their information. MCNA breached that duty by, among other things, failing to implement and maintain reasonable security

[38] https://www.sangfor.com/blog/cybersecurity/ransomware-attack-healthcare-mcna-dental-data-breach-affects-89m-patients#:~:text=According%20to%20TechCrunch%2C%20the%20LockBit,US%24%2010%20million%20ransom%20demand (last visited June 14, 2023).
[39] *Id.*

procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

C. MCNA Knew that Criminals Target PII/PHI

53. At all relevant times, Defendant knew, or should have known, its customers' patients', Plaintiffs', and all other Class Members' PII/PHI was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' PII/PHI from cyber-attacks that Defendant should have anticipated and guarded against.

54. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were 758 medical data breaches in 2020 with over 40 million patient records exposed.[40] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[41]

55. PII/PHI is a valuable property right.[42] The value of PII/PHI as a commodity is measurable.[43] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[44] American companies are estimated to have spent over $19 billion on acquiring

[40] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 15, 2021).
[41] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 15, 2021).
[42] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data
[43] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[44] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

personal data of consumers in 2018.[45] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

56. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

57. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[46] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[47] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[48]

58. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each

---

[45] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[46] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[47] *Id.*

[48] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

on the black market.[49] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[50]

59. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[51] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[52]

60. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[53]

61. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[49] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[50] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[51] *What Happens to Stolen Healthcare Data*, *supra* at n.10.
[52] *Id.*
[53] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

D. Theft of PII/PHI Has Grave and Lasting Consequences for Victims

62. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[54]

63. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[55] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[56]

64. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the

---

[54] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[55] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[56] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[57]

65. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[58]

66. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

67. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[59]

68. Theft of PII is even more serious when it includes theft of PHI. Data breaches

---

[57] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).
[58] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).
[59] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[60] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[61] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[62] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[63]

69. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

---

[60] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf

[61] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.14.

[62] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 15, 2021).

[63] *Id*.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[64]

70. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[65]

71. It is within this harsh and dangerous reality that Plaintiffs and all other Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

E. Damages Sustained by Plaintiffs and the Other Class Members

72. Plaintiffs and all other Class Members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

---

[64] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 24.
[65] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

CLASS ALLEGATIONS

73. Plaintiffs bring this action on behalf of themselves and the following classes:

> Nationwide Class: All residents of the United States who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.
>
> Alabama Subclass: All residents of Alabama who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.
>
> Massachussetts Subclass: All residents of Massachussetts who were notified by Defendant that their PHI and PII may have been compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class." The Alabama and Massachusetts Subclasses are referred to herein, collectively, as the "State Subclasses."

74. Excluded from the Class are: (1) the Judges presiding over the Action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or their parents, have a controlling interest, and their current or former officers and directors; (3) Persons who properly opt out; and (4) the successors or assigns of any such excluded Persons.

75. **Numerosity**: Class Members are so numerous that their individual joinder is impracticable, as the proposed class includes at least 8,923,662 members who are geographically dispersed.

76. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendant's uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

77. **Adequacy**: Plaintiffs' interests are aligned with the class they seek to represent and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and their

counsel intend to prosecute this action vigorously. The class's interests are well-represented by Plaintiffs and undersigned counsel.

78. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

79. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. Whether Defendant's conduct violated state consumer protection laws;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

c. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII/PHI;

d. Whether Defendant breached its duties to protect Plaintiffs' and Class Members' PII/PHI; and

e. Whether Plaintiffs and all other Class Members are entitled to damages and the measure of such damages and relief.

80. Given that Defendant engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

81. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

82. Defendant owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

83. Defendant knew the risks of collecting and storing Plaintiffs' and all other Class Members' PII/PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

75. Given the nature of Defendant's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

76. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class Members' PII/PHI.

77. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII/PHI to unauthorized individuals.

78. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and class Members, their PII/PHI would not have been compromised.

79. As a result of Defendant's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

80. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

81. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for

Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

82. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

83. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

84. Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

85. Plaintiffs and class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

86. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

87. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security

processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' PII/PHI to unauthorized individuals.

88. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

89. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

90. Plaintiffs and class Members gave MCNA their PII/PHI in confidence, believing that MCNA would protect that information. Plaintiffs and class Members would not have provided MCNA with this information had they known it would not be adequately protected. MCNA's acceptance and storage of Plaintiffs' and Class Members' PII/PHI created a fiduciary relationship between MCNA and Plaintiffs and class Members. In light of this relationship, MCNA must act

primarily for the benefit of people whose PII/PHI is provided to it, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

91. MCNA has a fiduciary duty to act for the benefit of Plaintiffs and class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class Members' PII/PHI that it collected.

92. As a direct and proximate result of MCNA's breaches of its fiduciary duties, Plaintiffs and class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in MCNA's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

93. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

94. In connection with receiving healthcare services and/or dental insurance coverage, Plaintiffs and all other Class Members entered into implied contracts with Defendant.

95. Pursuant to these implied contracts, Plaintiffs and Class Members paid money to Defendant, whether directly or through their healthcare providers, insurers, and/or state agencies and provided Defendant with their PII/PHI. In exchange, Defendant agreed to, among other things, and Plaintiffs understood that Defendant would: (1) provide dental and/or insurance services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' PII/PHI; and (3) protect Plaintiffs' and Class Members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

96. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as alleged above, Defendant recognized the importance of data security and the privacy of its customers' and serviced indiiduals' PII/PHI on its website and in its Privacy Notice. Had Plaintiffs and Class Members known that Defendant would not adequately protect their PII/PHI, they would not have entrused their PII/PHI to Defendant.

97. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Defendant with their PII/PHI and paid—directly or through their healthcare providers, insurers, and/or state agencies—for services from Defendant.

98. Defendant breached its obligations under its implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

99. Defendant's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

100. Plaintiffs and all other Class Members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or through their healthcare providers, insurers, and/or state agencies—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT V
Invasion of Privacy
(Intrusion Upon Seclusion)
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

101. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

102. Plaintiffs and Class Members had a reasonable expectation of privacy in the PII and PHI that Defendant disclosed without authorization.

103. By failing to keep Plaintiffs' and Class Members' PII and PHI safe and disclosing PHI and PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class members' privacy by, *inter alia*:

a. intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiffs' and Class Members' privacy by improperly using their PHI and PII properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure their PII and PHI from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiffs' and Class Members' PII and PHI without consent.

104. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

105. Defendant knew that its systems and processes for collecting, managing, storing, and protecting PII and PHI entrusted to it were vulnerable to data breaches prior to the Data Breach.

106. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their PII and PHI to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

107. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class members' reasonable expectations of privacy in their PII and PHI was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

108. In failing to protect Plaintiffs' and Class members' PII and PHI, and in disclosing that information, Defendant acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

109. Plaintiffs seek injunctive relief on behalf of the class, restitution, and all other damages available under this Count.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

110. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

111. This claim is pleaded in the alternative to the breach of implied contract claim.

112. Plaintiffs and class Members have both a legal and equitable interest in their PHI and PII that was collected by, stored by, and maintained by Defendant—thus conferring a benefit upon Defendant—that was ultimately compromised by the Data Breach.

113. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and class Members. Defendant also benefitted from the receipt of Plaintiffs' and Class Members' PHI and PII.

114. As a result of Defendant's failure to safeguard and protect Plaintiffs' PII and PHI, conduct, Plaintiffs and class Members suffered actual damages.

115. Defendant should not be permitted to retain the benefit belonging to Plaintiffs and class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that were mandated by federal, state, and local laws and industry standards.

116. Defendant should be compelled to provide for the benefit of Plaintiffs and class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VII
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the State Subclasses)

117. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

118. An actual controversy has arisen and exists between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand, concerning the Data Breach and Defendant's failure to protect Plaintiffs' and Class Members' PHI and PII, including with respect to the issue of whether Defendant took adequate measures to protect that information. Plaintiffs and class Members are entitled to judicial determination as to whether Defendant has performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiffs' and Class Members PHI and PII from unauthorized access, disclosure, and use.

119. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether they failed to adequately protect PHI and PII is necessary and appropriate to determine with certainty the rights of Plaintiffs and the Class Members, and so that there is clarity between the parties as to Defendant's data security obligations with respect to PHI and PII going forward, in view of the ongoing relationships between the parties.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class Members, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representatives and undersigned counsel as class counsel;

B. Award Plaintiffs and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: June 14, 2023

Respectfully submitted,

By: */s/ Mark B. DeSanto*

Mark B. DeSanto (FL Bar No. 107688)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

E. Michelle Drake (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Attorneys for Plaintiffs